PATENT OFFICE

JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: October 19, 1999

Application Number: Patent Application No. 11-296669

Applicant(s): CASIO COMPUTER CO., LTD.

April 7, 2000

Commissioner,

Patent Office Takahiko Kondo

Certificate No. 2000-3024160

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１０月１９日

出願番号
Application Number: 平成１１年特許願第２９６６６９号

出願人
Applicant (s): カシオ計算機株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ４月 ７日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号 出証特２０００－３０２４１６０

【書類名】　特許願
【整理番号】　A009906035
【提出日】　平成11年10月19日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 12/00
G09C 1/00
【発明の名称】　データベース管理装置、データベースシステム及び記録媒体
【請求項の数】　6
【発明者】
【住所又は居所】　東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
【氏名】　森　潤二
【発明者】
【住所又は居所】　東京都渋谷区本町１丁目６番２号　カシオ計算機株式会社内
【氏名】　黒澤　和大
【特許出願人】
【識別番号】　000001443
【氏名又は名称】　カシオ計算機株式会社
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9005919

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データベース管理装置、データベースシステム及び記録媒体

【特許請求の範囲】

【請求項１】　データベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化する第１の暗号化手段と、

この第１の暗号化手段による前記データベースの他の列項目のデータの暗号化に用いられた行鍵を各行に共通の別の鍵を用いて暗号化する第２の暗号化手段と、

前記第１の暗号化手段によって暗号化されたデータベースを前記第２の暗号化手段によって暗号化された行鍵と共に記憶する記憶手段と

を具備したことを特徴とするデータベース管理装置。

【請求項２】　前記行鍵は、前記データベースの各行に割り当てられた行番号と乱数とによって生成されることを特徴とする請求項１記載のデータベース管理装置。

【請求項３】　データベースを管理する第１の端末装置と、この第１の端末装置とは独立して前記データベースの検索を行う第２の端末装置とで構成されたデータベースシステムであって、

前記第１の端末装置側で、前記データベースを暗号化し、その暗号化データベースを可搬型の記録媒体に記録して配布し、

前記第２の端末装置側で、前記配布された記録媒体を用いて、そこに記録された暗号化データベースに対するデータ検索を行い、その検索結果として得られたデータを復号化して表示することを特徴とするデータベースシステム。

【請求項４】　前記第１の端末装置は、

前記データベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化すると共に、前記行鍵を各行に共通の別の鍵を用いて暗号化し、

この暗号化されたデータベースを前記暗号化後の行鍵と共に記録媒体に格納す

ることを特徴とする請求項３記載のデータベースシステム。

【請求項５】　前記記録媒体には、前記第１の端末装置にて暗号化されたデータベースと共にその暗号化データベースを検索するための所定のプログラムが格納されることを特徴とする請求項３記載のデータベースシステム。

【請求項６】　コンピュータに、

データベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化する第１の暗号化機能と、

この第１の暗号化機能による前記データベースの他の列項目のデータの暗号化に用いられた行鍵を各行に共通の別の鍵を用いて暗号化する第２の暗号化機能と

を実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データベースを暗号化して管理するデータベース管理装置、データベースを提供する端末とデータベース検索を行う端末とからなるデータベースシステム及びデータベースを暗号化するためのプログラムを記録した記録媒体に関する。

【０００２】

【従来の技術】

データベース管理装置では、データベースのセキュリティを確保するため、管理対象として保有しているデータベースを暗号化して保存しておくことが求められる。

【０００３】

ここで、データベースを暗号化する場合に、例えばパスワード等によって生成された１つの固定的な暗号化鍵を用いて対象ファイル全体を暗号化するのが一般的であった。

【０００４】

【発明が解決しようとする課題】

データベースは膨大なデータ量を有し、その中には機密性の高いデータ項目も含まれており、他のデータ項目よりもセキュリティを高くすることが要求される。しかしながら、上述したように従来の方式では、１つの固定的な暗号化鍵を用いて暗号化していたため、各データ項目のセキュリティレベルは同じになり、しかも、同じデータを持つ項目があった場合には暗号化結果も同じになってしまい、そこから暗号化鍵が解読される危険性があった。

【０００５】

本発明は前記のような課題を解決するためになされたもので、データベース上の特定のデータ項目に対するセキュリティを他のデータ項目よりも高めて暗号化することのできるデータベース管理装置、データベースシステム及び記録媒体を提供することを目的とする。

【０００６】

【課題を解決するための手段】

本発明は、データベースを暗号化する際に、検索に利用される列項目のデータについては当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては高セキュリティが要求される項目として各行毎に固有の行鍵を用いて暗号化し、さらに前記行鍵を各行に共通の別の鍵を用いて暗号化するようにしたものである。

【０００７】

具体的には、本発明のデータベース管理装置は、データベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化する第１の暗号化手段と、この第１の暗号化手段による前記データベースの他の列項目のデータの暗号化に用いられた行鍵を各行に共通の別の鍵を用いて暗号化する第２の暗号化手段と、前記第１の暗号化手段によって暗号化されたデータベースを前記第２の暗号化手段によって暗号化された行鍵と共に記憶する記憶手段とで構成される。

【０００８】

このような構成によれば、データベースを暗号化する際に、検索に利用される

所定の列項目以外の列項目のデータについては、各行毎に鍵を異ならせて暗号化することで、その列項目の中に同じ値のデータがあっても、異なる値として暗号化結果を得ることができ、しかも、当該列項目の暗号化に用いられた鍵（行鍵）を別の鍵で再暗号化することで、鍵の解読を困難として高セキュリティ化を実現できる。

【０００９】

また、前記データベースの各行に割り当てられた行番号と乱数とによって前記行鍵を生成するようにすれば、鍵の解読がさらに困難となり、セキュリティを強化することができる。

【００１０】

また、データベースを管理する第１の端末装置と、この第１の端末装置とは独立して前記データベースの検索を行う第２の端末装置とでデータベースシステムを構築することも可能である。

【００１１】

このデータベースシステムでは、第１の端末装置側にて前記データベースを暗号化し、その暗号化データベースを記録媒体に記録して配布し、第２の端末装置側にて前記配布された記録媒体を用いて、そこに記録された暗号化データベースに対するデータ検索を行い、その検索結果として得られたデータを復号化して表示する。この場合、前記のようにデータベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては各行毎に固有の行鍵を用いて暗号化すると共に、前記行鍵を各行に共通の別の鍵を用いて暗号化することで、記録媒体にデータベースを格納して配布したとしても、そのセキュリティを確保することができる。

【００１２】

【発明の実施の形態】

以下、図面を参照して本発明の実施形態を説明する。

【００１３】

（第１の実施形態）

図１は本発明の第１の実施形態に係るデータベース管理装置の構成を示す図で

ある。本装置は、行と列からなるマトリクス形式のデータベースを暗号化して管理する機能と共に、その暗号化されたデータベースを検索する機能を備えたものであって、例えば磁気ディスク等の記録媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されるコンピュータによって実現される。

【００１４】

図１に示すように、本装置には、ＣＰＵ１１、表示装置１２、入力装置１３、プログラム記憶装置１４、鍵生成装置１５、データ記憶装置１６、データベースＩ／Ｆ１７が設けられている。

【００１５】

ＣＰＵ１１は、本装置全体の制御を行うものであり、プログラム記憶装置１４に記憶されたプログラムを読み込み、そのプログラムに従って各種処理を実行する。本実施形態において、ＣＰＵ１１は図８に示すようなデータベースの暗号化処理や、図９及び図１０に示すようなデータベースの検索処理を実行する。

【００１６】

表示装置１２は、データを表示するためのデバイスであり、例えばＬＣＤ（Liquid Crystal Display）やＣＲＴ（Cathode-ray tube）等が用いられる。入力装置１３は、データを入力するためのデバイスであり、例えばキーボード、マウス等が用いられる。

【００１７】

プログラム記憶装置１４は、例えばＲＯＭあるいはＲＡＭなどで構成され、本装置に必要なプログラムを記憶する。本装置に必要なプログラムとしては、データベース暗号化プログラムやデータベース検索プログラム等がある。

【００１８】

なお、プログラム記憶装置１４は半導体メモリの他に磁気的、光学的記録媒体で構成することができる。この記録媒体はＣＤ-ＲＯＭ等の可搬型の媒体やハードディスク等の固定的な媒体を含む。また、この記録媒体に格納するプログラムは、その一部若しくは全部をサーバやクライアントからネットワーク回線などの伝送媒体を介して伝送制御部から受信する構成にしてもよく、更に、前記記録媒体はネットワーク上に構築されたサーバの記録媒体であってもよい。更に、前記

プログラムをネットワーク回線などの伝送媒体を介してサーバーやクライアントへ伝送してこれらの機器にインストールするように構成してもよい。

【００１９】

鍵生成装置１５は、データベースの暗号化に用いられる暗号化鍵を生成するためのデバイスであり、ここでは暗号化鍵として基本鍵、行鍵、列鍵の３つの鍵を生成するための基本鍵生成部１５ａ、行鍵生成部１５ｂ、列鍵生成部１５ｃから構成されている。

【００２０】

データ記憶装置１６は、本装置に必要な各種のデータやテーブルを記憶するためのデバイスであり、例えばＲＡＭあるいは磁気ディスク装置等の外部記憶装置で構成される。このデータ記憶装置１６には、基本鍵パラメータテーブル１６ａ、基本鍵記憶部１６ｂ、鍵スペックテーブル１６ｃ、暗号化データ格納部１６ｄ、検索文字列格納部１６ｅが設けられている。

【００２１】

基本鍵パラメータテーブル１６ａは、基本鍵のパラメータ値が登録されたテーブルである（図４参照）。基本鍵記憶部１６ｂは、オペレータの指定操作によって得られた基本鍵のパラメータ値を記憶する。鍵スペックテーブル１６ｃは、データベースの各列（フィールド）毎に定義された暗号化方式の種類（非暗号化，行鍵，列鍵）を記憶するテーブルである（図６参照）。暗号化データ格納部１６ｄは、暗号化されたデータベースを格納する。検索文字列格納部１６ｅは、データベース検索時にオペレータにより指定された検索用文字列を格納する。

【００２２】

データベースＩ／Ｆ１７は、本装置とは独立して設けられた外部データベース記憶装置１８との間でデータの授受を行うためのインタフェースである。この外部データベース記憶装置１８は、複数のデータベースファイル（オリジナルデータ）を有しており、これらのデータベースファイルは本装置からのアクセスによって選択的に読み出されるように構成されている。

【００２３】

ここで、本装置の動作を説明する前に、理解を容易にするため、本装置におけ

るデータベースの暗号化方法について説明しておく。

【００２４】

データベースを暗号化する場合に、各行毎（レコード毎）に異なる鍵を用いて暗号化すれば鍵の解読は困難となり、セキュリティ性を高めることができる。しかし、すべての行について鍵を異ならせると、データベースを検索する際に、暗号化されているデータを各行毎の鍵で復号化するか、または、検索用として入力されたデータ（キーワード）を各行毎の鍵で暗号化しなければならいため、検索結果を得るのに時間がかかることになる。一方、各列毎（フィールド毎）に異なる鍵を用いてデータベースを暗号化すると、検索対象となる列項目に対応した鍵のみを用いて検索用データを暗号化すれば良いのでデータベース検索を高速に行うことができる。しかし、同じ列の中で同一のデータがあると、暗号化結果も同じになってしまうため、そこから鍵を解読される可能性が高くなる。

【００２５】

そこで、本発明では、データベースを暗号化する際に、検索に頻繁に利用される列項目のデータについては非暗号化あるいはその列項目に共通の鍵（列鍵）で暗号化し、その他の列項目のデータについては高セキュリティが要求される項目として、各行毎に異なる鍵（行鍵）で暗号化し、さらに、各行毎に異なる鍵（行鍵）を各行に共通の別の鍵（基本鍵）で再暗号化することを特徴とする。つまり、高セキュリティが要求される列項目のデータについては、各行毎に暗号化鍵を異ならせ、さらに、その暗号化鍵をシステム基本鍵で暗号化することで、高セキュリティ化を実現するものである。

【００２６】

図１１に具体例を示す。

【００２７】

図１１は本装置によるデータベースの構成を説明するための図であり、図１１（ａ）は暗号化前の状態、同図（ｂ）は暗号化後の状態、同図（ｃ）は復号化後の状態を示している。

【００２８】

図１１（ａ）に示すように、本装置では、行と列からなるマトリックス形式の

データベースを暗号化対象としている。ここでは、個人データをデータベース化したものを示している。このデータベースには、「ｃｏｄｅ」，「ｎａｍｅ」，「ｓｔａｔｅ」，「ａｇｅ」，「ｐｈｏｎｅ」の各列項目（フィールド）を有する。

【００２９】

このようなデータベースに対し、列鍵と行鍵を用いて暗号化を行う。すなわち、検索に頻繁に利用される列項目を「ｓｔａｔｅ」，「ａｇｅ」とした場合に、これらの列項目の各行のデータ（レコード）については、各列項目に共通の列鍵を用いて暗号化し、その他の列項目「ｎａｍｅ」，「ｐｈｏｎｅ」の各行のデータ（レコード）については高セキュリティが要求される項目として、各行毎に固有の行鍵を用いて暗号化してレコードファイルに格納する。その際に、当該列項目の暗号化に用いられた行鍵を基本鍵で再暗号化し、その暗号化された行鍵を各レコードに付加して格納する。なお、「ｃｏｄｅ」の列項目のデータについては暗号化を行わないものとする。

【００３０】

図１１（ａ）のデータベースを列鍵と行鍵を用いて暗号化した結果を図１１（ｂ）に示す。この場合、「ｌｉｎｅ　ｋｅｙ」といった列項目が追加され、そこに基本鍵で暗号化された行鍵（９６５８，９１４３，８２７８…）が格納される。図１に示すデータ記憶装置１６の暗号化データ格納部１６ｄには、図１１（ｂ）に示すような状態でデータベースが保存されることになる。

【００３１】

また、データベースを検索する場合には、検索に利用される列項目に対応した列鍵を用いて検索用データを暗号化してから検索処理を行う。例えば、「ｓｔａｔｅ」の中の「Ｆｌｏｒｉｄａ」といったデータを検索する場合には、まず、検索用データとして入力された「Ｆｌｏｒｉｄａ」を「ｓｔａｔｅ」の列鍵で暗号化して、「ｈ＊／ｆＤＤ」を得る。この「ｈ＊／ｆＤＤ」といったデータを「ｓｔａｔｅ」の列の各行から検索する。これにより、「ｃｏｄｅ２」と「ｃｏｄｅ８」に該当するデータが存在することがわかる。

【００３２】

また、暗号化されたデータベースを元に戻す場合には、暗号化の時と同じ列鍵、行鍵、基本鍵を用いる。図１１（ｂ）のデータベースを暗号化の時と同じ列鍵、行鍵、基本鍵を用いて復号化すると、図１１（ｃ）に示すように元のデータを得ることができる。

【００３３】

次に、このようなデータベースの暗号化／復号化を実現するための具体的な構成について説明する。

【００３４】

図２は本装置の構成を機能的に示したブロック図である。

【００３５】

本装置を機能的に示すと、入力処理系は基本鍵指定部２１、基本鍵設定部２２、鍵スペック入力部２３、鍵スペック設定部２４で構成される。また、暗号化処理系はデータ読出し部２５、レコード入力メモリ２６、暗号化処理部２７、暗号化レコード書込メモリ２８、データ書込み部２９で構成され、復号化処理系は暗号化レコード読出メモリ３０、復号化処理部３１、レコード出力メモリ３２、データ出力部３３で構成される。また、この他に、上述した基本鍵パラメータテーブル１６ａ、基本鍵記憶部１６ｂ、鍵スペックテーブル１６ｃ、暗号化データ格納部１６ｄが用いられる。基本鍵パラメータテーブル１６ａは基本鍵設定部２２に用いられ、基本鍵記憶部１６ｂ、鍵スペックテーブル１６ｃ、暗号化データ格納部１６ｄは暗号化処理部２７及び復号化処理部３１の両方に用いられる。

【００３６】

なお、図２に示した各種のメモリ２６，２８，３０，３２は、レジスタ群であり、例えばデータ記憶装置１６の所定のエリアに設けられる。

【００３７】

このような構成において、データベースの暗号化を行う場合には、まず、オペレータの操作により基本鍵指定部２１を通じて基本鍵を指定する。基本鍵設定部２２は、この基本鍵指定部２１によって指定された基本鍵のパラメータ値を基本鍵パラメータテーブル１６ａから読み出して基本鍵記憶部１６ｂにセットする。

【００３８】

具体的には、図３に示すような基本鍵設定ダイアログを通じて基本鍵の指定を行う。基本鍵設定ダイアログは、オペレータが基本鍵を任意に指定するための画面であり、その画面上に基本鍵指定ボタン部４１、ＯＫボタン４２、キャンセルボタン４３が設けられている。基本鍵指定ボタン部４１は複数個のボタンからなり、オペレータがこれらのボタンの中の任意のボタンを押下すると、その押下したボタンの位置により基本鍵のパラメータ値が決定される。なお、ＯＫボタン４２は基本鍵の指定を確定するためのボタン、キャンセルボタン４３は基本鍵の指定を取り消すためのボタンである。

【００３９】

例えば、基本鍵指定ボタン部４１に１６個のボタン「１」～「１６」が左から４個ずつ順に配列されているものとする。図４に示すように、基本鍵パラメータテーブル１６ａには、これらのボタンの位置に対応させて基本鍵のパラメータ値が定義されている。オペレータが基本鍵指定ボタン部４１上の「１」のボタンを押下すると、この基本鍵パラメータテーブル１６ａに従って基本鍵のパラメータ値として「５」が決定される。同様に、基本鍵指定ボタン部４１上の「２」のボタンを押下した場合には、基本鍵のパラメータ値として「７」が決定される。

【００４０】

次に、外部データベース記憶装置１８にアクセスして、外部データベース記憶装置１８に格納された各種データベースの中から暗号化対象となるデータベースを指定する。データベースの指定後、オペレータの操作により鍵スペック入力部２３を通じて当該データベースの各データ項目に対する鍵スペックを指定する。鍵スペック設定部２４は、この鍵スペック入力部２３による鍵スペックの指定操作に従って鍵スペックテーブル１６ｃに鍵スペック情報の登録を行う。

【００４１】

具体的には、図５に示すような鍵スペック設定ダイアログを通じて鍵スペックの指定を行う。鍵スペック設定ダイアログは、オペレータがデータベースの各列項目（フィールド）毎に暗号化方式（暗号化に用いる鍵の種類）を任意に指定するための画面であり、その画面上に暗号化方式指定欄５１、ＯＫボタン５２、キャンセルボタン５３が設けられている。

【００４２】

暗号化方式としては、各行毎に固有の鍵（行鍵）を用いた暗号化、各列毎に共通の鍵（列鍵）を用いた暗号化がある。ここでは、非暗号化を含め、０：非暗号化、１：行鍵、２：列鍵として、暗号化方式指定欄５１にデータベースの各列項目に対する暗号化方式を数値入力するように構成されている。なお、ＯＫボタン５２は鍵スペックの指定を確定するためのボタン、キャンセルボタン５３は鍵スペックの指定を取り消すためのボタンである。この鍵スペック設定ダイアログにて暗号化方式を指定すると、その指定内容が各列項目に対する鍵スペック情報として鍵スペックテーブル１６ｃに登録される。

【００４３】

図６に鍵スペックテーブル１６ｃの登録例を示す。

【００４４】

ここでは、データベースの列番号「１」の項目に対して非暗号化、列番号「２」の項目に対して行鍵、列番号「３」の項目に対して列鍵、列番号「４」の項目に対して列鍵、列番号「５」の項目に対して行鍵が登録されている。列番号「１」の項目は「ｃｏｄｅ」、列番号「２」の項目は「ｎａｍｅ」、列番号「３」の項目は「ｓｔａｔｅ」、列番号「４」の項目は「ａｇｅ」、列番号「５」の項目は「ｐｈｏｎｅ」に相当する。

【００４５】

このようにして、基本鍵記憶部１６ｂに基本鍵が設定され、鍵スペックテーブル１６ｃに各列項目に対する鍵スペック情報が設定されると、これらの設定情報を用いてデータベースの暗号化が以下のような手順で実行される。

【００４６】

すなわち、図２に示すように、まず、外部データベース記憶装置１８の中から指定されたデータベースがデータ読出し部２５によって行単位（レコード単位）で読み出され、レコード入力メモリ２６に順に格納される。暗号化処理部２７はこのレコード入力メモリ２６に格納されたレコードを基本鍵パラメータテーブル１６ａ及び基本鍵記憶部１６ｂを用いて暗号化する。このときの暗号化処理については後に図７を参照して詳しく説明する。

【００４７】

暗号化処理部２７にて暗号化されたレコードは暗号化レコード書込メモリ２８に格納された後、データ書込み部２９を通じて暗号化データ格納部１６ｄに書き込まれる。このようにして、暗号化データ格納部１６ｄ内に暗号化されたデータベースが作成される。

【００４８】

一方、データベースの復号化は暗号化と逆の手順で行なわれる。

【００４９】

すなわち、まず、暗号化データ格納部１６ｄに格納された暗号化データベースが行単位（レコード単位）で読み出され、暗号化レコード読出メモリ３０に順に格納される。復号化処理部３１は、この暗号化レコード読出メモリ３０に格納された暗号化レコードを鍵スペックテーブル１６ｃ及び基本鍵記憶部１６ｂを用いて復号化する。このときの復号化処理については後に図７を参照して詳しく説明する。復号化処理部３１にて復号化されたレコードはレコード出力メモリ３２に格納された後、データ出力部３３を通じてデータファイル３４に出力される。このようにして、データファイル３４内に復号化されたデータベースが作成される。なお、データファイル３４は図１のデータ記憶装置１６の所定のエリアに設けられる。

【００５０】

図７に具体例を示す。

【００５１】

図７は本装置におけるデータベースの暗号化時と復号化時のデータの流れを示す図である。

【００５２】

今、暗号化対象として指定されたデータベースの１行目のレコードがデータ読出し部２５によって読み出され、レコード入力メモリ２６に格納されたとする。この場合、図１１（ａ）に示すデータベースを例にすると、そのデータベースの１行目の「１００１」，「Ｊｈｏｎ」，「Ｎｅｗ　Ｙｏｒｋ」，「２２」，「４０７－２２８－６６１１」といった５項目からなるデータが順にレコード入力メ

モリ２６に格納されることになる。

【００５３】

暗号化処理部２７は、この５項目のデータからなるレコードに対し、鍵スペックテーブル１６ｃを参照して各項目に応じた暗号化を行う。例えば、鍵スペックテーブル１６ｃに設定された内容が図６のような場合には、列番号「１」に相当する当該レコードの１項目（「ｃｏｄｅ」）のデータについては暗号化せずに、そのまま暗号化レコード書込メモリ２８に書き込む。

【００５４】

また、列番号「２」に相当する当該レコードの２項目（「ｎａｍｅ」）のデータについては行鍵を用いて暗号化して暗号化レコード書込メモリ２８に書き込む。行鍵は当該行番号と乱数によってランダムに生成されるものであり、各行毎に異なる値を有する。列番号「３」に相当する当該レコードの３項目（「ｓｔａｔｅ」）のデータについては列鍵を用いて暗号化する。この列鍵は各列に共通の値を有する。

【００５５】

同様にして、列番号「４」に相当する当該レコードの４項目（「ａｇｅ」）のデータについては列鍵、列番号「５」に相当する当該レコードの５項目（「ｐｈｏｎｅ」）のデータについては行鍵を用いて、それぞれ暗号化して暗号化レコード書込メモリ２８に書き込む。これにより、暗号化レコード書込メモリ２８には、「１００１」，「ｗｊｌｓ」，「ｎｏｅｖｊｏｌｃ」，「ｊｈ」，「ｊｇｄｌｔｙｔｆｈＤＳｋ」といった１行分の暗号化データが生成されることになる。

【００５６】

さらに、暗号化処理部２７は、基本鍵記憶部１６ｂにセットされたパラメータ値を用いて各行に共通の基本鍵にて当該レコードの暗号化に用いた行鍵を暗号化することにより、その暗号化後の行鍵を暗号化レコード書込メモリ２８に付加する。図７の例では、「９５６８」といったデータが暗号化後の行鍵である。

【００５７】

以上のような処理がデータベースの各行に対して繰り返し行われ、暗号化後のデータベースが暗号化データ格納部１６ｄに格納される。この状態が図１１（ｂ

）に相当する。

【００５８】

一方、復号化時には、暗号化時と逆の処理になる。

【００５９】

すなわち、暗号化データ格納部１６ｄに格納された暗号化データベースが１レコード単位で暗号化レコード読出メモリ３０に読み出される。今、１行目の暗号化レコードが暗号化レコード読出メモリ３０に読み出されたとする。前記の例であれば、「１００１」，「ｗｊｌｓ」，「ｎｏｅｖｊｏｌｃ」，「ｊｈ」，「ｊｇｄｌｔｙｔｆｈＤＳｋ」及び「９５６８」といった行鍵を含む６項目からなる暗号化データが順に暗号化レコード読出メモリ３０に格納されることになる。

【００６０】

復号化処理部３１は、この６項目のデータからなるレコードに対し、鍵スペックテーブル１６ｃを参照して各項目に応じた復号化を行う。図６の例では、列番号「１」に相当する当該レコードの１項目（「ｃｏｄｅ」）のデータについては非暗号化であるため、そのままレコード出力メモリ３２に書き込む。

【００６１】

また、列番号「２」に相当する当該レコードの２項目（「ｎａｍｅ」）のデータについては行鍵を用いて復号化してレコード出力メモリ３２に書き込む。ただし、行鍵については暗号化時に基本鍵にて暗号化されているため、その基本鍵を用いて行鍵自体を復号化して元に戻す処理が必要となる。また、列番号「３」に相当する当該レコードの２項目（「ｎａｍｅ」）のデータについては列鍵を用いて復号化してレコード出力メモリ３２に書き込む。

【００６２】

同様にして、列番号「４」に相当する当該レコードの４項目（「ａｇｅ」）のデータについては列鍵、列番号「５」に相当する当該レコードの５項目（「ｐｈｏｎｅ」）のデータについては行鍵を用いて、それぞれ復号化してレコード出力メモリ３２に書き込む。これにより、レコード出力メモリ３２には、「１００１」，「Ｊｈｏｎ」，「Ｎｅｗ　Ｙｏｒｋ」，「２２」，「４０７－２２８－６６１１」といった１行分の復号化データ（元データ）が生成されることになる。

【００６３】

以上のような処理が暗号化データベースの各行に対して繰り返し行われ、復号化後のデータベースがデータファイル３４に格納される。この状態が図１１（ｃ）に相当する。

【００６４】

以下、フローチャートを参照して本装置の動作について説明する。

【００６５】

ここでは、（ａ）データベースを暗号化する場合の処理と、（ｂ）データベースを検索する場合の処理に分けて説明する。なお、このフローチャートで示す各機能を実現するプログラムはＣＰＵが読み取り可能なプログラムコードの形態で前記プログラム記憶装置１４の記録媒体に格納されている。また、このプログラムはプログラムコードの形態でネットワーク回線などの伝送媒体を介して伝送することもできる。

【００６６】

（ａ）データベースを暗号化する場合

図８は本装置にて実行されるデータベース暗号化処理の動作を示すフローチャートである。今、データベースが暗号化されていない状態で外部データベース記憶装置１８に記憶されているものとする。この状態が図１１（ａ）である。

【００６７】

データベースの暗号化を行う場合に、まず、図８（ａ）のフローチャートに示すように、基本鍵の設定を行う（ステップＡ１１）。この基本鍵の設定は、上述したように基本鍵設定ダイアログを通じて行う。

【００６８】

すなわち、図８（ｂ）のフローチャートに示すように、データベースの暗号化時に図３に示すような基本鍵設定ダイアログが表示装置１２に表示される（ステップＢ１１）。この基本鍵設定ダイアログには、基本鍵指定ボタン部４１が設けられており、オペレータはその基本鍵指定ボタン部４１に配列された複数個のボタンの中の任意のボタンを押下することで基本鍵の指定を行う。

【００６９】

オペレータが基本鍵指定ボタン部４１の中の任意のボタンを押下した後、ＯＫボタン５２を押下して確定指示を行うと（ステップＢ１２）、当該ボタンの位置に対応した基本鍵のパラメータ値が図４に示す基本鍵パラメータテーブル１６ａから読み出されて基本鍵記憶部１６ｂにセットされる（ステップＢ１３）。

【００７０】

次に、暗号化対象となるデータベースを指定する（ステップＡ１２）。本実施形態では、本装置とは独立した外部データベース記憶装置１８に各種のデータベース（元データ）を保持している。したがって、暗号化を行う場合には、データベースＩ／Ｆ１７を介して外部データベース記憶装置１８にアクセスし、その中から暗号化対象となるデータベースを指定するといった操作が必要となる。

【００７１】

暗号化対象となるデータベースを指定後、そのデータベースに設けられた各列項目の中で検索に利用する列項目と、暗号化を必要としない列項目をそれぞれ設定すると共に（ステップＡ１３）、各列項目に対する暗号化鍵（行鍵と列鍵）を決定する（ステップＡ１４）。

【００７２】

これらの設定は、上述した図５の鍵スペック設定ダイアログを通じて行う。この鍵スペック設定ダイアログは、オペレータがデータベースの各列項目（フィールド）毎に暗号化方式（暗号化に用いる鍵の種類）を任意に指定するための画面であり、前記ステップＡ１２にて、暗号化対象となるデータベースを指定した際に表示装置１２に表示される。ここでは、非暗号化を含め、０：非暗号化、１：行鍵、２：列鍵として、前記図５の鍵スペック設定ダイアログに設けられた暗号化方式指定欄５１にデータベースの各列項目に対する暗号化方式を数値入力するように構成されている。

【００７３】

この場合、図１１（ａ）に示すデータベースにおいて、検索に利用される列項目（つまり、高セキュリティが要求されない項目）は３列目の「ｓｔａｔｅ」と４列目の「ａｇｅ」であり、これらの列項目に対しては列鍵を指定し、その他の項目である２列目の「ｎａｍｅ」と５列目の「ｐｈｏｎｅ」は高セキュリティが

要求される項目として行鍵を指定するものとする。また、暗号化を必要としない列項目は１列目の「ｃｏｄｅ」である。ここで設定された暗号化鍵は、鍵スペック情報として鍵スペックテーブル１６ｃに図６のように登録される。

【００７４】

このような設定操作の後、データベースの暗号化が以下のようにして実行される。

【００７５】

すなわち、まず、データベースの各行のデータが第１行目から順に図２に示すレコード入力メモリ２６に読み出される（ステップＡ１５）。その際、鍵生成装置１５の行鍵生成部１５ｂによって当該行に割り付けられた行番号と乱数により行鍵がランダムに生成され、データ記憶装置１６の所定のエリアに保持される（ステップＡ１６）。

【００７６】

ここで、レコード入力メモリ２６に読み出された行データの各列項目が１列目から順次に指定され（ステップＡ１７）、その指定された列項目に対する暗号化方式が鍵スペックテーブル１６ｃに記憶された鍵スペック情報に基づいて判断され（ステップＡ１８）、行鍵または列鍵を用いて暗号化される（ステップＡ１９～Ａ２２）。

【００７７】

具体的に説明すると、データベースの中の１列目の項目である「ｃｏｄｅ」については図６の鍵スペックテーブル１６ｃに示すように非暗号化項目として設定されているので、何もしない（ステップＡ１８→Ａ２３）。つまり、「ｃｏｄｅ」の項目は元データのままである。

【００７８】

また、２列目の項目である「ｎａｍｅ」については行鍵が設定されているので、前記ステップＡ１６にて生成された当該行番号に対応した行鍵（各行毎に固有の鍵）がデータ記憶装置１６の所定エリアから読み出され（ステップＡ１８→Ａ２１）、その行鍵にて２列目のデータが暗号化される（ステップＡ２２）。

【００７９】

また、３列目の項目である「ｓｔａｔｅ」については列鍵が設定されているので、当該列番号に対応した列鍵（各列毎に共通の鍵）が鍵生成装置１５の列鍵生成部１５ｃにより生成され（ステップＡ１８→Ａ１９）、その列鍵にて３列目のデータが暗号化される（ステップＡ２０）。

【００８０】

以下同様にして、４列目の項目である「ａｇｅ」については列鍵にて暗号化が行われ、５列目の項目である「ｐｈｏｎｅ」については行鍵にて暗号化が行われることになる。

【００８１】

暗号化された各列項目のデータは、図２の暗号化レコード書込メモリ２８に格納される。ここで、最終項目の暗号化が終了した時点で、当該行データの２列目及び３列目の項目の暗号化に用いられた行鍵が基本鍵にて暗号化されて暗号化レコード書込メモリ２８に追加される（ステップＡ２５）。この基本鍵は、鍵生成装置１５の基本鍵生成部１５ａにて生成される。基本鍵生成部１５ａは、前記図３の基本鍵設定ダイアログにてオペレータが指定したパラメータ値を基本鍵記憶部１６ｂから読み出し、そのパラメータ値に基づいて基本鍵を生成する。

【００８２】

暗号化レコード書込メモリ２８に１行分の暗号化データと、行鍵を基本鍵にて暗号化したデータが格納されると、それらのデータが暗号化データ格納部１６ｄに保存される（ステップＡ２５）。

【００８３】

このような暗号化処理がデータベースの各行毎について繰り返し行なわれる（ステップＡ２６→Ａ１５）。すべての行のデータの暗号化処理が終了し、最終的に得られた暗号化データベースの状態が図１１（ｂ）である。この暗号化データベースには、各行の最終項目に行鍵が基本鍵にて暗号化された状態で付加されている。

【００８４】

（ｂ）データベースを検索する場合

次に、暗号化後のデータベースを検索する処理について説明する。

【００８５】

図９は本装置にて実行されるデータベース検索処理の動作を示すフローチャートである。今、前記（ａ）で説明した暗号化処理にて、データベースが暗号化されて暗号化データ格納部１６ｄに保存されているものとする。

【００８６】

まず、図９（ａ）のフローチャートに示すように、図示せぬデータベース検索用設定画面にて、検索情報の入力を行う（ステップＣ１１）。検索情報の入力とは、検索対象となる列項目と、検索用の文字列（キーワード）を入力することである。これらの入力情報はデータ記憶装置１６の所定のエリアに格納される。入力装置１３を通じて検索情報が入力されると、検索前処理が実行される（ステップＣ１２）。

【００８７】

この検索前処理では、図９（ｂ）のフローチャートに示すように、検索対象として入力された列項目が所定の列項目であるか否かが判断され（ステップＤ１１）、所定の列項目であることが判明した場合には（ステップＤ１１のＹｅｓ）、その列項目に共通の列鍵で検索用の文字列が暗号化される（ステップＤ１２）。

【００８８】

所定の列項目とは、前記データベースの暗号化時に設定された検索対象項目（検索に利用される項目つまり高セキュリティが要求されない項目）であり、具体的には「ｓｔａｔｅ」，「ａｇｅ」の各項目が該当する。この検索対象項目には列鍵が設定されている。したがって、前記ステップＤ１１では、鍵スペックテーブル１６ｃを参照して当該列項目に設定された鍵の種類によって所定の列項目であるか否かの判断を行うことになる。所定の列項目であれば、鍵生成装置１５の列鍵生成部１５ｃにより当該列項目に対応した列鍵を生成し、その列鍵にて検索用の文字列を暗号化することになる。

【００８９】

また、検索対象として入力された列項目が所定の列項目でなかった場合には（ステップＤ１１のＮｏ）、前記のような検索用文字列の暗号化は行われない。

【００９０】

このような検索前処理の後、データベースの検索処理（図１０参照）が行われ（ステップＣ１３）、その検索結果として得られたデータが表示装置１２に表示される（ステップＣ１４）。図１０にデータベースの検索処理を示す。

【００９１】

図１０は前記ステップＣ１３の検索処理の動作を具体的に示すフローチャートである。

【００９２】

まず、図１０（ａ）のフローチャートに示すように、検索用文字列がデータベースとの比較文字列としてデータ記憶装置１６の検索文字列格納部１６ｅにセットされる（ステップＥ１１）。この場合、上述したように検索対象として入力された列項目が所定の列項目（「ｓｔａｔｅ」，「ａｇｅ」）であった場合には、前記検索前処理によって、当該検索用文字列がその列項目に対応した列鍵にて暗号化されて検索文字列格納部１６ｅにセットされる。その他の列項目の場合には、暗号化されることなく、そのままの状態で検索文字列格納部１６ｅにセットされる。

【００９３】

次に、データ記憶装置１６のデータベース格納エリア１６ａに格納された暗号化データベースの列番号による暗号化方式が判断される（ステップＥ１２）。その結果、検索対象が列鍵で暗号化された所定の列項目に該当する場合には、その対象列の各行データが順次走査され（ステップＥ１２→Ｅ１３）、それらの行の暗号化文字列と前記検索文字列格納部１６ｅにセットされた検索用文字列（暗号化された文字列）とが比較される（ステップＥ１４）。

【００９４】

この比較処理では、図１０（ｂ）のフローチャートに示すように、データベースから取り出された当該行の暗号化文字列と検索用の暗号化文字列とを比較して、両者が一致するか否かを判断する（ステップＦ１１）。両者が一致した場合には（ステップＦ１１のＹｅｓ）、その一致した項目を含むレコードデータをデータベース検索結果として抽出する（ステップＦ１２）。

【００９５】

この処理を暗号化データベースの終端まで繰り返して、該当するデータを順次抽出し（ステップＥ１５）、この抽出したデータを検索結果として出力する（ステップＥ２１）。

【００９６】

具体的に説明すると、図１１（ｂ）の暗号化データベースの例で、例えば「ｓｔａｔｅ」の項目の中の「Ｆｌｏｒｉｄａ」といったデータを検索することが指定された場合には、まず、検索用データとして入力された「Ｆｌｏｒｉｄａ」を「ｓｔａｔｅ」の３列目の列鍵で暗号化して「ｈ＊／ｆＤＤ」を得る。この「ｈ＊／ｆＤＤ」といったデータを「ｓｔａｔｅ」の列から検索する。これにより、コード番号の「１００１」と「１００８」に該当するデータが存在することがわかる。

【００９７】

一方、検索対象が行鍵で暗号化された列項目つまり高セキュリティが要求される列項目に該当する場合には、その対象列の各行データが順次走査される（ステップＥ１２→Ｅ１６）。ここで、これらの行データの暗号化に用いられた各行鍵は基本鍵にて暗号化されているので、各行鍵を基本鍵にて復号化するといった処理が必要となる（ステップＥ１７）。各行鍵が基本鍵にて復号化されると、それらの行鍵を用いて各行の暗号化文字列が復号化され（ステップＥ１８）、その復号化の文字列と前記検索文字列格納部１６ｅにセットされた検索用文字列（非暗号化文字列）とが比較される（ステップＥ１９）。

【００９８】

この比較処理では、図１０（ｂ）のフローチャートに示すように、データベースから取り出された当該行の復号化文字列と検索用の非暗号化文字列との比較により、両者が一致するか否かを判断する（ステップＦ１１）。両者が一致した場合には（ステップＦ１１のＹｅｓ）、その一致した項目を含むレコードデータをデータベース検索結果として抽出する（ステップＦ１２）。

【００９９】

この処理を暗号化データベースの終端まで繰り返して、該当するデータを順次抽出し（ステップＥ２０）、この抽出したデータを検索結果として出力する（ス

テップＥ２１）。

【０１００】

具体的に説明すると、図１１（ｂ）の暗号化データベースの例で、例えば「ｎａｍｅ」の項目の中の「Ｊｈｏｎ」といったデータを検索することが指定された場合には、まず、「ｎａｍｅ」の１行目に対応した行鍵「９６５４」（暗号化データ）を基本鍵にて復号化した後、その行鍵を用いて１行目の「ｗＪＩＳ」を復号化して「Ｊｈｏｎ」といったデータを得る。同様にして、各行に対応した行鍵（暗号化データ）を基本鍵にて復号化した後、その行鍵を用いて各行目のデータを復号化して元のデータを得る。図１１（ｃ）に示すように「ｎａｍｅ」の項目の各行のデータを各行鍵にて復元した後、その中から検索用データとして入力された「Ｊｈｏｎ」と一致するデータを検索する。これにより、コード番号の「１００１」に該当するデータが存在することがわかる。

【０１０１】

このように、データベースを暗号化する際に、検索に利用される所定の列項目については列共通鍵で暗号化することで、検索時には、検索用データをその列共通鍵で暗号化してデータベース上の暗号化データと比較して高速検索を実現できる。また、所定の列項目以外の列項目については各行毎に異なる鍵を与えて暗号化と、さらに、その行鍵を基本鍵にて暗号化しておくことで、鍵の解読を困難として高セキュリティ化を実現できるものである。

【０１０２】

（第２の実施形態）

前記第１の実施形態では、本発明を装置単体で構成したが、データベース管理を行う端末とデータベース検索を行う端末とに分けて、これらの端末でデータベースシステムを構築することも可能である。

【０１０３】

以下に、このようなデータベースシステムについて説明する。

【０１０４】

図１２は本発明の第２の実施形態に係るデータベースシステムの構成を示すブロック図である。本システムは、１台のサーバ装置１００と複数台（ここでは３

台のみ示す）の携帯端末２００ａ，２００ｂ，２００ｃ…とで構成される。サーバ装置１００と各携帯端末２００ａ，２００ｂ，２００ｃ…との間はオフラインであり、データの授受は記録媒体４００ａ，４００ｂ，４００ｃ…を通じて行われる。

【０１０５】

サーバ装置１００は、データベースサービスを行うサーバコンピュータとして用いられるものであって、各端末に配布するデータの収集処理を行う配布データ収集装置１０１、データベースの暗号化処理を行う暗号化装置１０２、各種アプリケーションソフト（ＡＰ）を格納したＡＰソフト格納部１０３、各種のデータベースを格納したデータベース格納部１０４を備えている。ＡＰソフト格納部１０３及びデータベース格納部１０４は、例えば磁気ディスク装置等のデータ記憶装置によって構成される。この他、サーバ装置１００には、特に図示しないが、汎用コンピュータに標準装備されている表示装置、入力装置等も設けられている。

【０１０６】

一方、携帯端末２００ａ，２００ｂ，２００ｃ…は、サーバ装置１００からデータベースの提供を受けるクライアントコンピュータとして用いられるものである。携帯端末２００ａは、暗号化されたデータベースを復号化処理する復号化装置２０１ａ、データベース検索処理を行うデータベース検索装置２０２ａを備えている。携帯端末２００ｂ，２００ｃについても同様の構成であり、それぞれに復号化装置２０１ｂ，２０１ｃ、データベース検索装置２０２ｂ，２０２ｃを備えている。また、携帯端末２００ａ，２００ｂ，２００ｃには、特に図示しないが、表示装置、入力装置等の他、媒体読込み装置も設けられている。これらの携帯端末２００ａ，２００ｂ，２００ｃ…は、オンライン上でデータを閲覧するためのブラウザ機能を備えておらず、サーバ装置１００との間のデータの授受はすべて記録媒体４００ａ，４００ｂ，４００ｃ…を通じて行うように構成されている。

【０１０７】

記録媒体４００ａ，４００ｂ，４００ｃ…は、例えばＣＦカード（コンパクト

フラッシュメモリカード）からなる可搬型の記録媒体である。カードリーダ／ライタ３００は、これらの記録媒体４００ａ，４００ｂ，４００ｃ…に対するデータの書込みや読出しを行うためのデバイスであり、サーバ装置１００に接続されている。

【０１０８】

このような構成において、サーバ装置１００側では、データベース格納部１０４内の各種データベースの中でオペレータが指定したデータベースを読み込み、暗号化装置１０２を通じて暗号化する。この場合、暗号化装置１０２では、前記第１の実施形態と同様の手法によりデータベースの暗号化する。すなわち、検索に利用される所定の列項目については列共通鍵で暗号化すると共に、所定の列項目以外の列項目については高セキュリティが要求される項目として、各行毎に異なる鍵を与えて暗号化し、さらに、その行鍵を基本鍵にて暗号化するといった処理を行う。

【０１０９】

ここで、暗号化装置１０２によって暗号化されたデータベースをファイルに保存し、この暗号化ファイルを例えばＣＦカード等の可搬型記録媒体４００ａ，４００ｂ，４００ｃ…にカードリーダ／ライタ３００を用いて格納する。この場合、記録媒体４００ａ，４００ｂ，４００ｃ…に暗号化ファイルを格納する際に、図１３に示すように、暗号化データファイル４０２の他に、鍵スペックテーブル４０３、基本鍵パラメータテーブル４０４、さらにアプリケーションプログラム４０１も格納しておく。

【０１１０】

鍵スペックテーブル４０３は、データベースの各列（フィールド）毎に定義された暗号化方式の種類（非暗号化，行鍵，列鍵）を記憶したテーブルであり、前記第１の実施形態における鍵スペックテーブル１６ｃと同様の構成を有する（図６参照）。基本鍵パラメータテーブル４０４は、基本鍵のパラメータ値が登録されたテーブルであり、前記第１の実施形態における基本鍵パラメータテーブル１６ａと同様の構成を有する（図４参照）。この鍵スペックテーブル４０３及び基本鍵パラメータテーブル４０４は、暗号化装置１０２内に保持されていたもので

ある。また、アプリケーションプログラム４０１は、データベース検索用のプログラムであり、ＡＰソフト格納部１０３内に保持されていたものである。

【０１１１】

これらの情報が格納された記録媒体４００ａ，４００ｂ，４００ｃ…は、携帯端末２００ａ，２００ｂ，２００ｃ…を扱う各ユーザにそれぞれ配布される。各ユーザは、配布された記録媒体４００ａ，４００ｂ，４００ｃ…を自身が持つ端末に挿入することで、データ検索を行うことができる。

【０１１２】

すなわち、例えば携帯端末２００ａであれば、配布された記録媒体４００ａを挿入することで、その記録媒体４００ａに記録されていたデータ検索用のアプリケーションプログラム４０１、暗号化データファイル４０２の他に、鍵スペックテーブル４０３、基本鍵パラメータテーブル４０４を読み込む。そして、データ検索用のアプリケーションプログラム４０１を起動し、所望の列項目を指定して、暗号化データファイル４０２に対するデータ検索を行い、その検索結果として得られたデータを復号化して表示する。

【０１１３】

データ検索は、携帯端末２００ａに設けられたデータベース検索装置２０２ａにて行われる。このデータベース検索装置２０２ａは、データ検索用のアプリケーションプログラム４０１に従って動作し、前記第１の実施形態と同様のデータベース検索処理を実行する。また、データの復号化は、復号化装置２０１ａにて行われる。この復号化装置２０１ａは、鍵スペックテーブル４０３及び基本鍵パラメータテーブル４０４を参照して、前記第１の実施形態と同様のデータベース復号化処理を実行する。

【０１１４】

このように、データベース管理を行う端末とデータベース検索を行う端末とに分けてデータベースシステムを構築するようにすれば、例えば顧客管理用のデータベースを暗号化して記録媒体に記録し、これを営業マンに配布し、営業マンは別の端末を用いてデータ検索を行うといったような利用が可能となる。この場合、記録媒体に記録されたデータベースは上述したような手法にて暗号化されてい

るため、そのデータの機密性を保持することができる。また、記録媒体には、暗号化ファイルだけでなく、データ検索用のアプリケーションプログラムも格納されている。したがって、携帯端末側にはデータ検索用のアプリケーションプログラムを搭載しておく必要はなく、簡易な構成の携帯端末で本システムを実現できるといった利点がある。

【０１１５】

【発明の効果】

以上詳記したように本発明によれば、データベースを暗号化する際に、検索に利用される所定の列項目以外の列項目のデータについては、各行毎に鍵を異ならせて暗号化し、さらに、当該列項目の暗号化に用いられた鍵を別の鍵で再暗号化するようにしたため、鍵の解読を困難として高セキュリティ化を実現することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係るデータベース管理装置の構成を示す図。

【図２】

前記データベース管理装置の構成を機能的に示したブロック図。

【図３】

前記データベース管理装置における基本鍵設定ダイアログの構成を示す図。

【図４】

前記データベース管理装置における基本鍵パラメータテーブルの一例を示す図。

【図５】

前記データベース管理装置における鍵スペック設定ダイアログの構成を示す図。

【図６】

前記データベース管理装置における鍵スペックテーブルの登録例を示す図。

【図７】

前記データベース管理装置におけるデータベースの暗号化時と復号化時のデー

タの流れを示す図。

【図８】

前記データベース管理装置にて実行されるデータベース暗号化処理の動作を示すフローチャート。

【図９】

前記データベース管理装置にて実行されるデータベース検索処理の動作を示すフローチャート。

【図１０】

前記図９のステップＣ１３の検索処理の動作を具体的に示すフローチャート。

【図１１】

前記データベース管理装置におけるデータベースの構成を説明するための図であり、図１１（ａ）は暗号化前の状態、同図（ｂ）は暗号化後の状態、同図（ｃ）は復号化後の状態を示す図。

【図１２】

本発明の第２の実施形態に係るデータベースシステムの構成を示すブロック図。

【図１３】

前記データベースシステムに用いられる記録媒体のデータ内容を示す図。

【符号の説明】

１１…ＣＰＵ

１２…表示装置

１３…入力装置

１４…プログラム記憶装置

１５…鍵生成装置

１５ａ…基本鍵生成部

１５ｂ…行鍵生成部

１５ｃ…列鍵生成部

１６…データ記憶装置

１６ａ…基本鍵パラメータテーブル

１６ｂ…基本鍵記憶部

１６ｃ…鍵スペックテーブル

１６ｄ…暗号化データ格納部

１６ｅ…検索文字列格納部

１７…データベースＩ／Ｆ

１８…外部データベース記憶装置

１００…サーバ装置

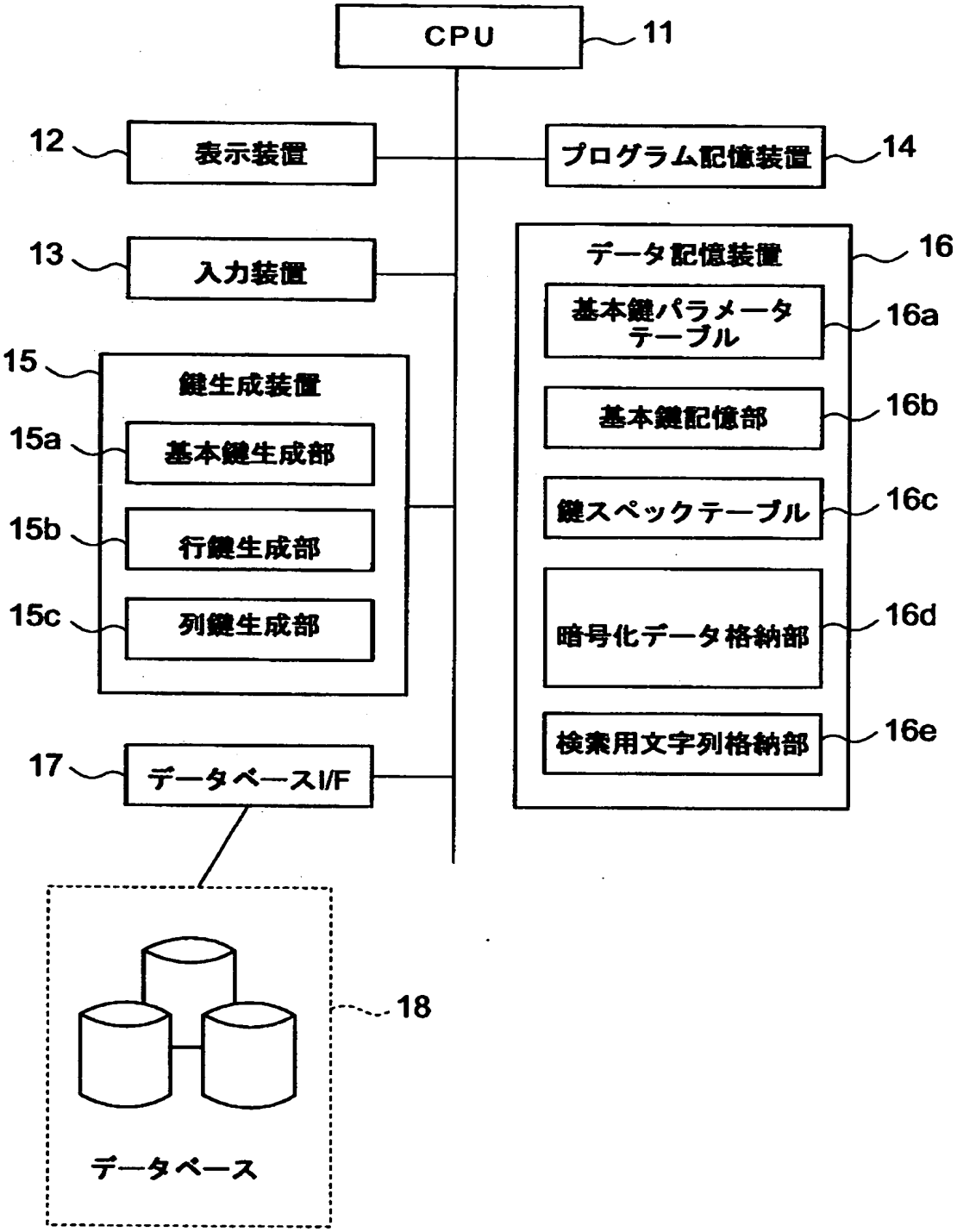
２００ａ～２００ｃ…携帯端末

３００…カードリーダ／ライタ

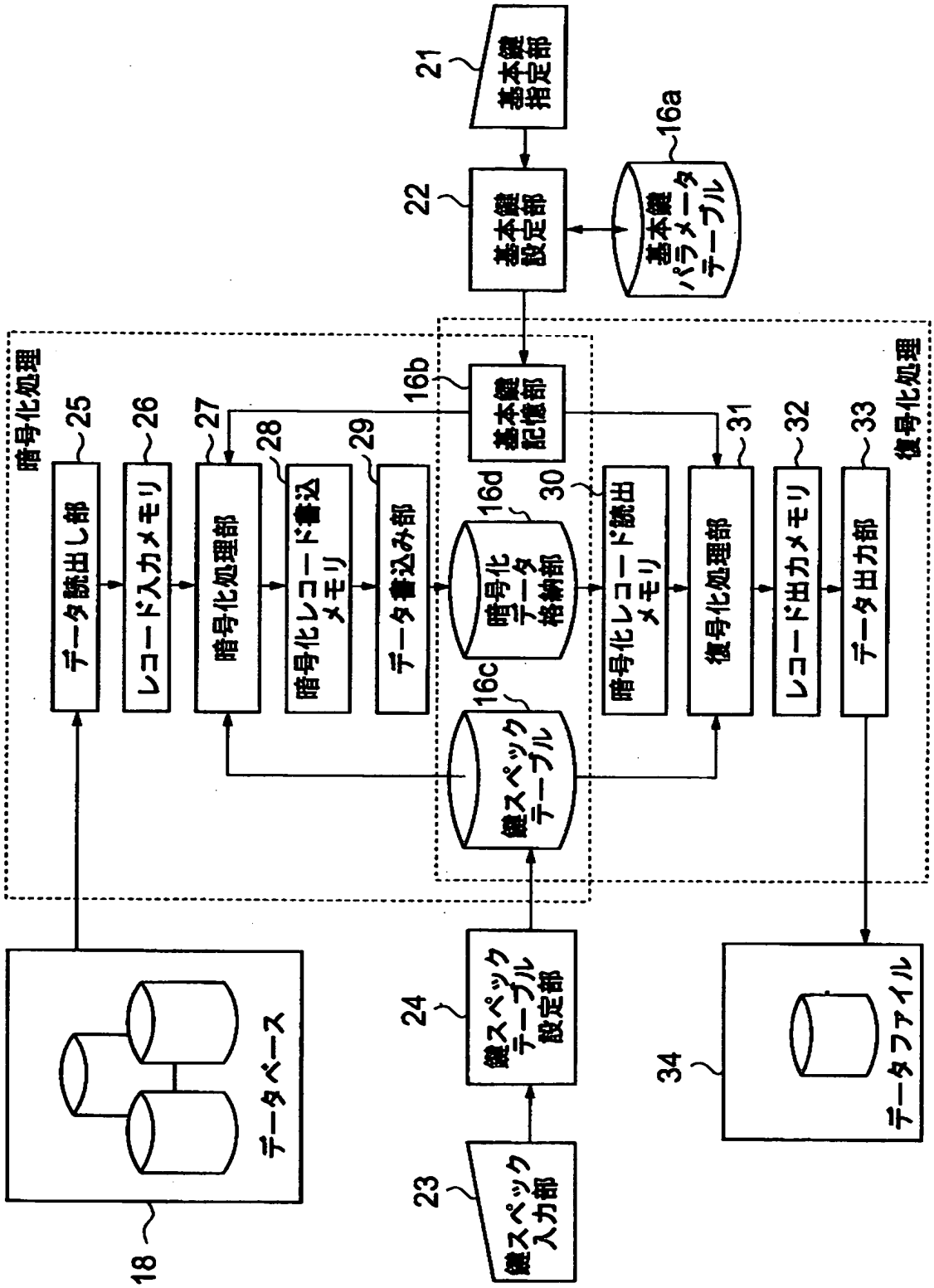
４００ａ～４００ｃ…記録媒体

【書類名】　図面

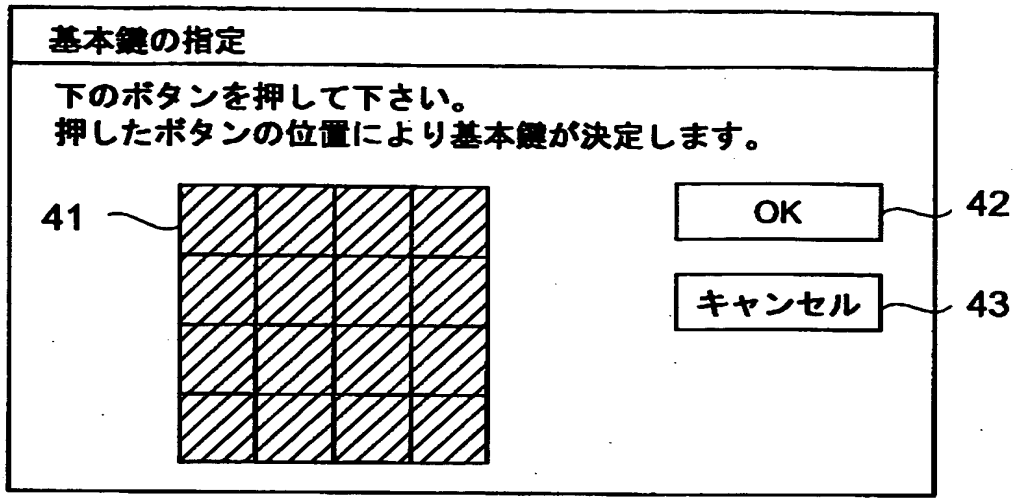
【図１】


CPU
11
12
表示装置
プログラム記憶装置
14
13
入力装置
データ記憶装置
16
基本鍵パラメータテーブル
16a
15
鍵生成装置
基本鍵記憶部
16b
15a
基本鍵生成部
鍵スペックテーブル
16c
15b
行鍵生成部
暗号化データ格納部
16d
15c
列鍵生成部
検索用文字列格納部
16e
17
データベースI/F
18
データベース

【図２】


暗号化処理
復号化処理
21
基本鍵指定部
22
基本鍵設定部
16a
基本鍵パラメータテーブル
16b
基本鍵記憶部
25
データ読出し部
26
レコード入力メモリ
27
暗号化処理部
28
暗号化レコード書込メモリ
29
データ書込み部
16d
暗号化データ格納部
30
暗号化レコード読出メモリ
31
復号化処理部
32
レコード出力メモリ
33
データ出力部
16c
鍵スペックテーブル
18
データベース
24
鍵スペックテーブル設定部
23
鍵スペック入力部
34
データファイル

【図３】

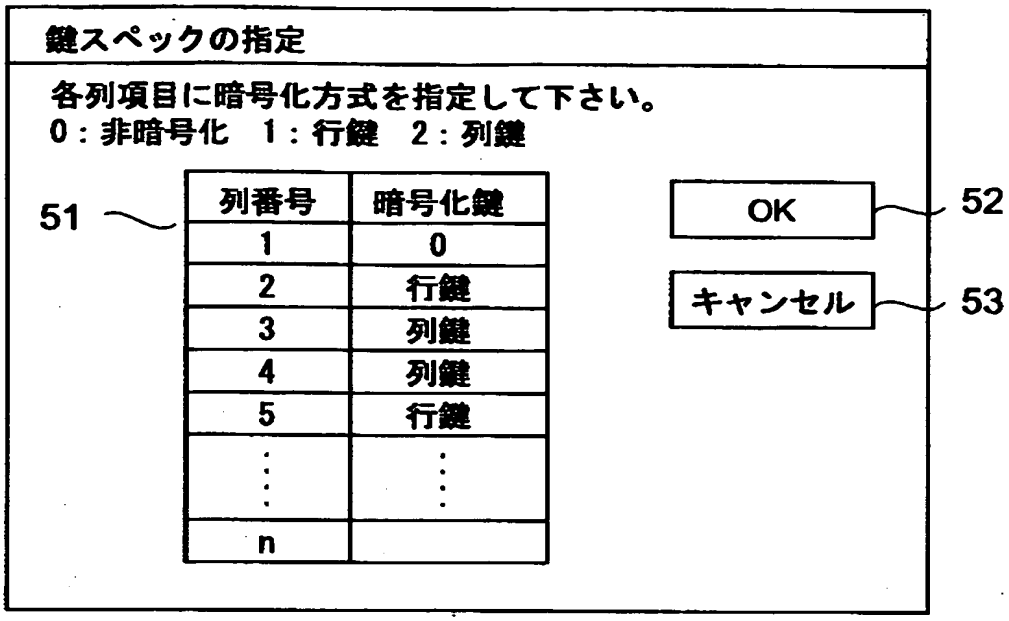


【図４】

基本鍵パラメータテーブル　16a

ボタン位置	パラメータ値
1	5
2	7
3	9
4	11
5	13
6	15
7	17
8	19
9	21
10	23
11	25
12	27
13	29
14	31
15	33
16	35

【図５】

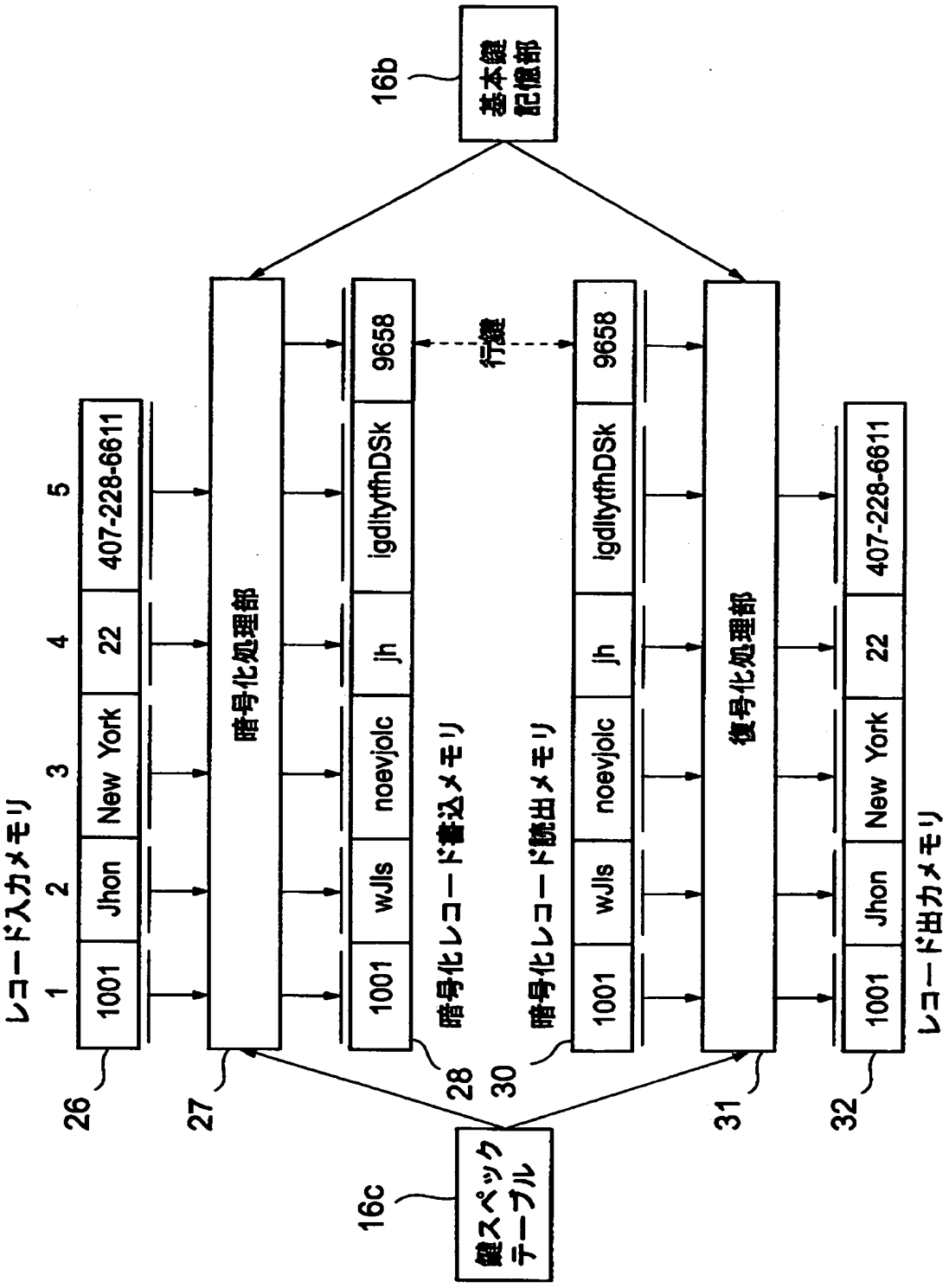


【図６】

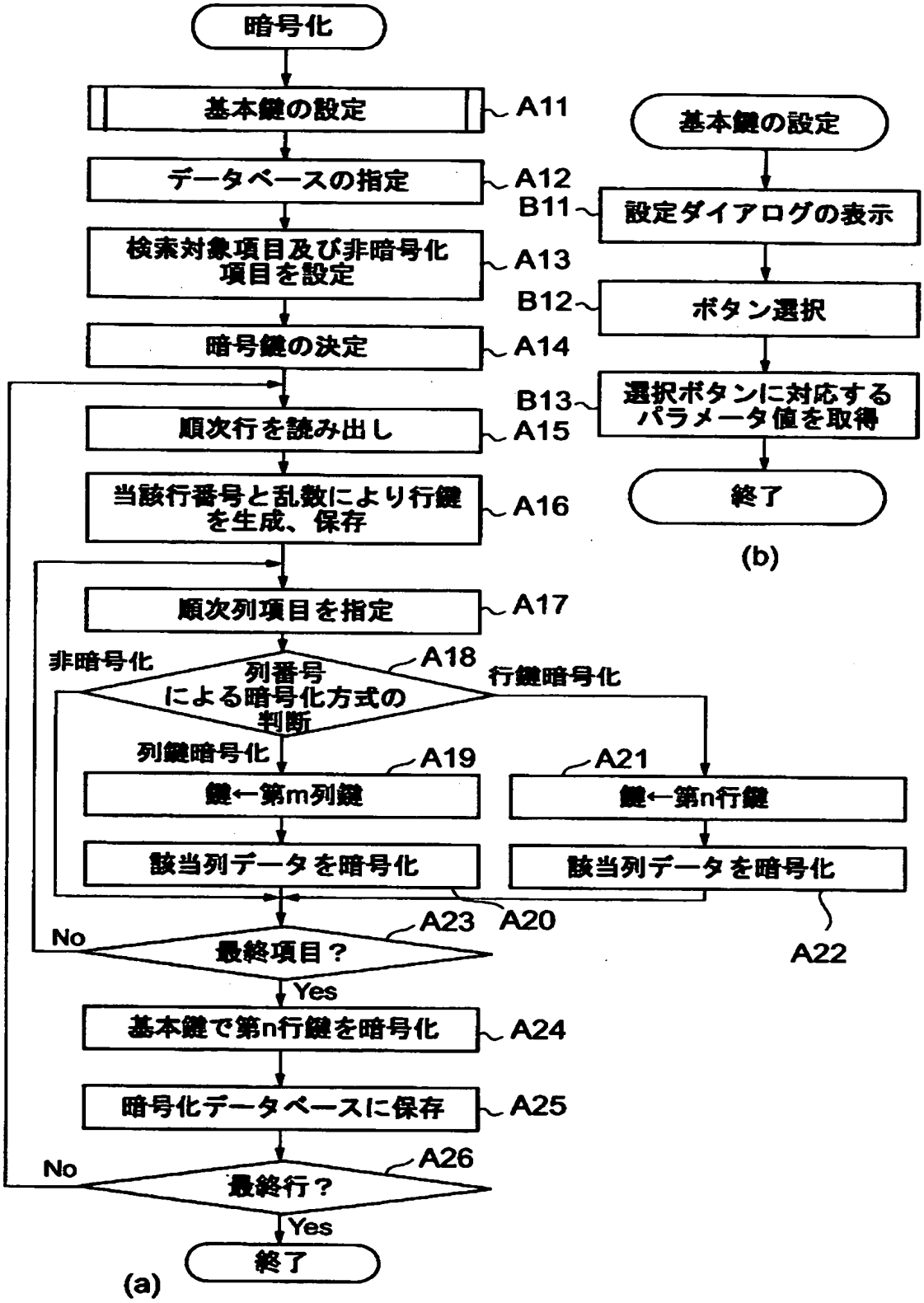
鍵スペックテーブル　16c

列名前	列番号	暗号化鍵
(code)	1	0
(name)	2	行鍵
(state)	3	列鍵
(age)	4	列鍵
(phone)	5	行鍵

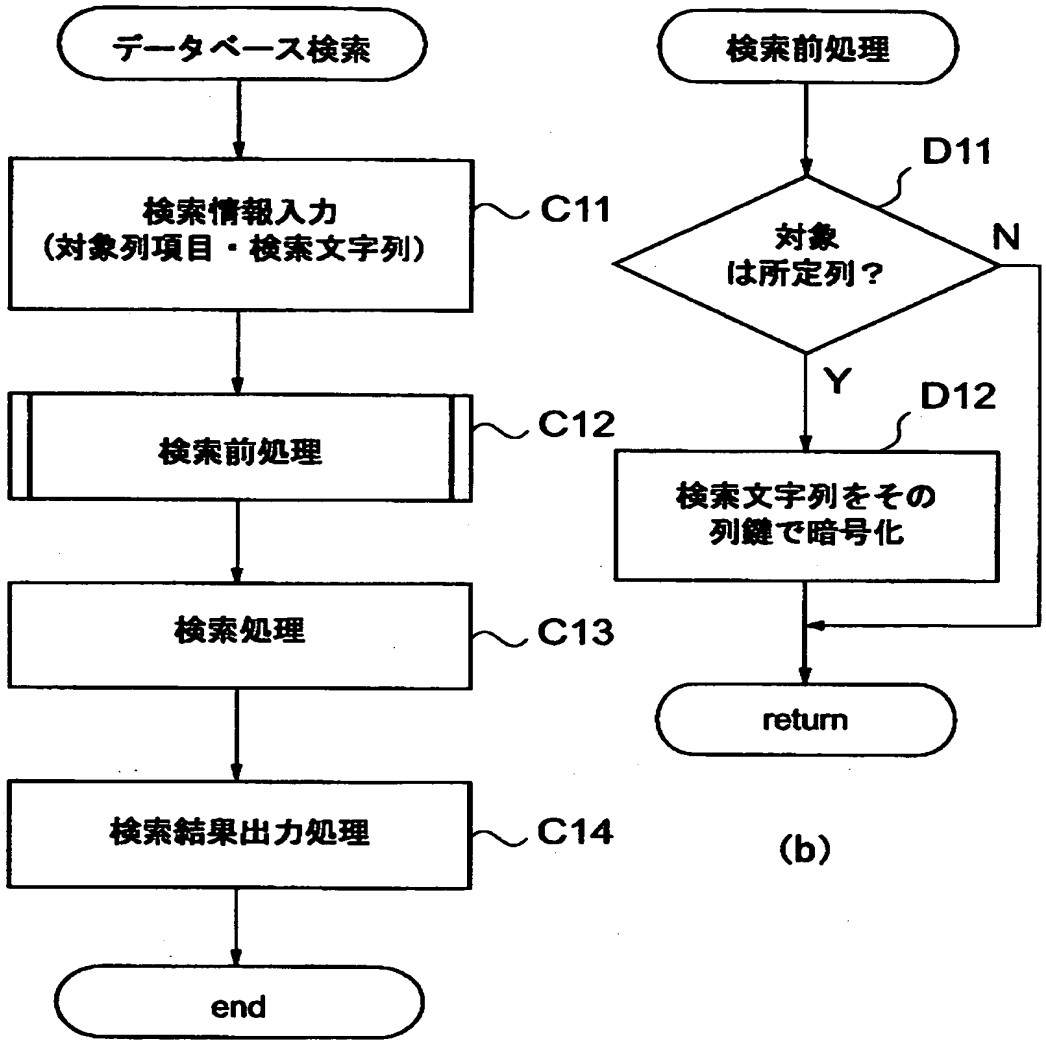
【図７】


16b
基本鍵記憶部
暗号化処理部
復号化処理部
行鍵
暗号化レコード書込メモリ
暗号化レコード読出メモリ
レコード入力メモリ
レコード出力メモリ
1
2
3
4
5
1001
Jhon
New York
22
407-228-6611
1001
wJls
noevjolc
jh
igdltyfhDSk
9658
26
27
28
30
31
32
16c
鍵スペックテーブル

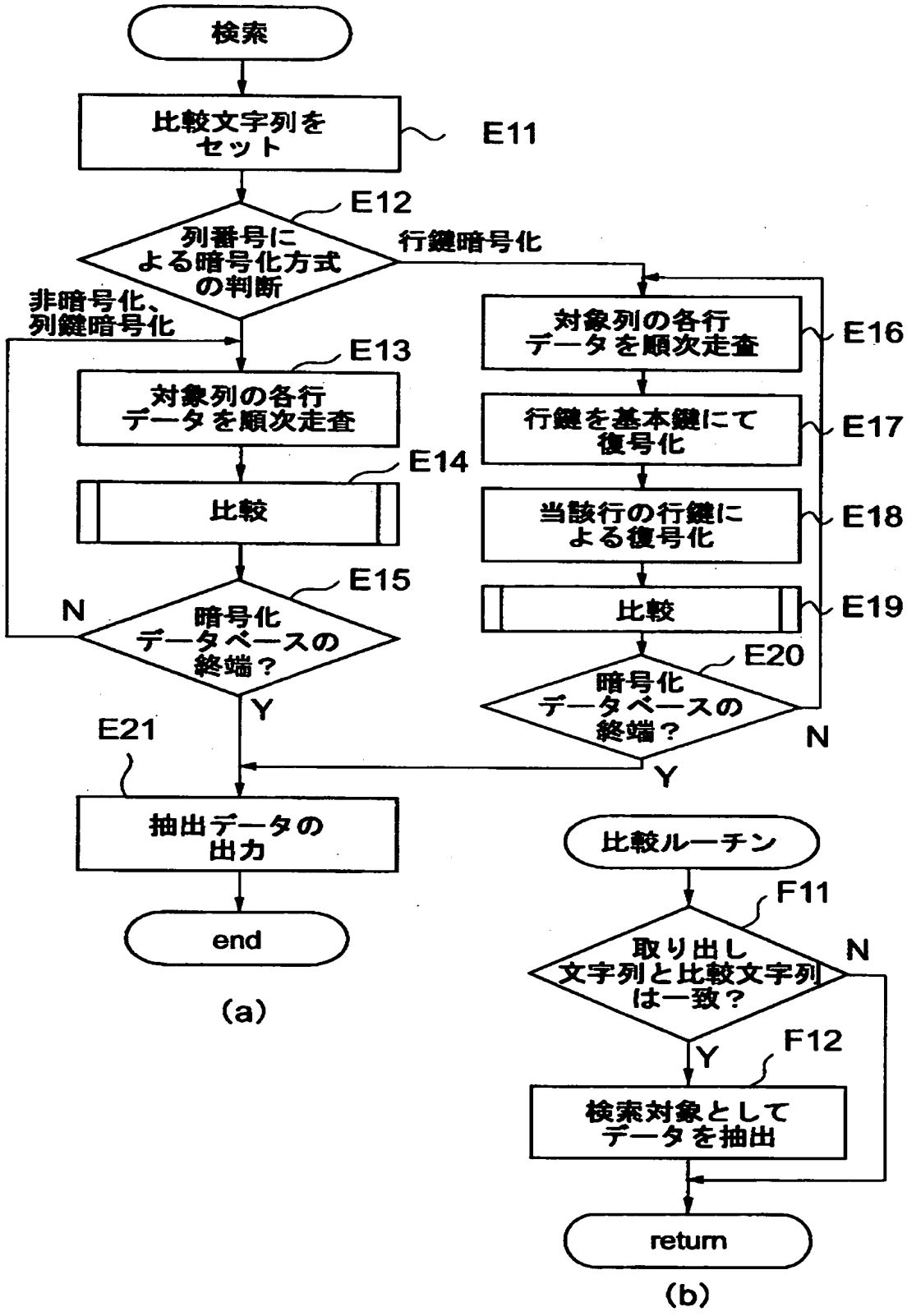
【図８】


暗号化
基本鍵の設定
A11
データベースの指定
A12
検索対象項目及び非暗号化項目を設定
A13
暗号鍵の決定
A14
順次行を読み出し
A15
当該行番号と乱数により行鍵を生成、保存
A16
順次列項目を指定
A17
非暗号化
列番号による暗号化方式の判断
A18
行鍵暗号化
列鍵暗号化
A19
鍵←第m列鍵
該当列データを暗号化
A21
鍵←第n行鍵
該当列データを暗号化
A20
A22
No
最終項目？
A23
Yes
基本鍵で第n行鍵を暗号化
A24
暗号化データベースに保存
A25
No
最終行？
A26
Yes
終了
(a)
基本鍵の設定
B11
設定ダイアログの表示
B12
ボタン選択
B13
選択ボタンに対応するパラメータ値を取得
終了
(b)

【図９】


データベース検索
検索情報入力
(対象列項目・検索文字列)
C11
検索前処理
C12
検索処理
C13
検索結果出力処理
C14
end
(a)
検索前処理
D11
対象
は所定列？
N
Y
D12
検索文字列をその
列鍵で暗号化
return
(b)

【図１０】


検索
比較文字列をセット
E11
E12
列番号による暗号化方式の判断
行鍵暗号化
非暗号化、列鍵暗号化
E13
対象列の各行データを順次走査
E14
比較
E15
暗号化データベースの終端？
N
Y
E21
抽出データの出力
end
(a)
E16
対象列の各行データを順次走査
E17
行鍵を基本鍵にて復号化
E18
当該行の行鍵による復号化
E19
比較
E20
暗号化データベースの終端？
N
Y
比較ルーチン
F11
取り出し文字列と比較文字列は一致？
N
Y
F12
検索対象としてデータを抽出
return
(b)

【図１１】

(a)

code	name	state	age	phone
1001	Jhon	New York	22	407-228-6611
1002	Chris	Florida	21	123-456-7890
1003	Michael	Minnesota	27	101-202-3030
1004	David	Iowa	34	523-761-0045
1005	Mark	New York	30	832-962-9001
1006	Daniel	Iowa	25	231-981-9454
1007	George	Idaho	31	561-545-4389
1008	Henry	Florida	22	239-203-9800
1009	Joe	New Jersey	27	239-129-9898

暗号化 ↓ 列鍵 行鍵

(b)

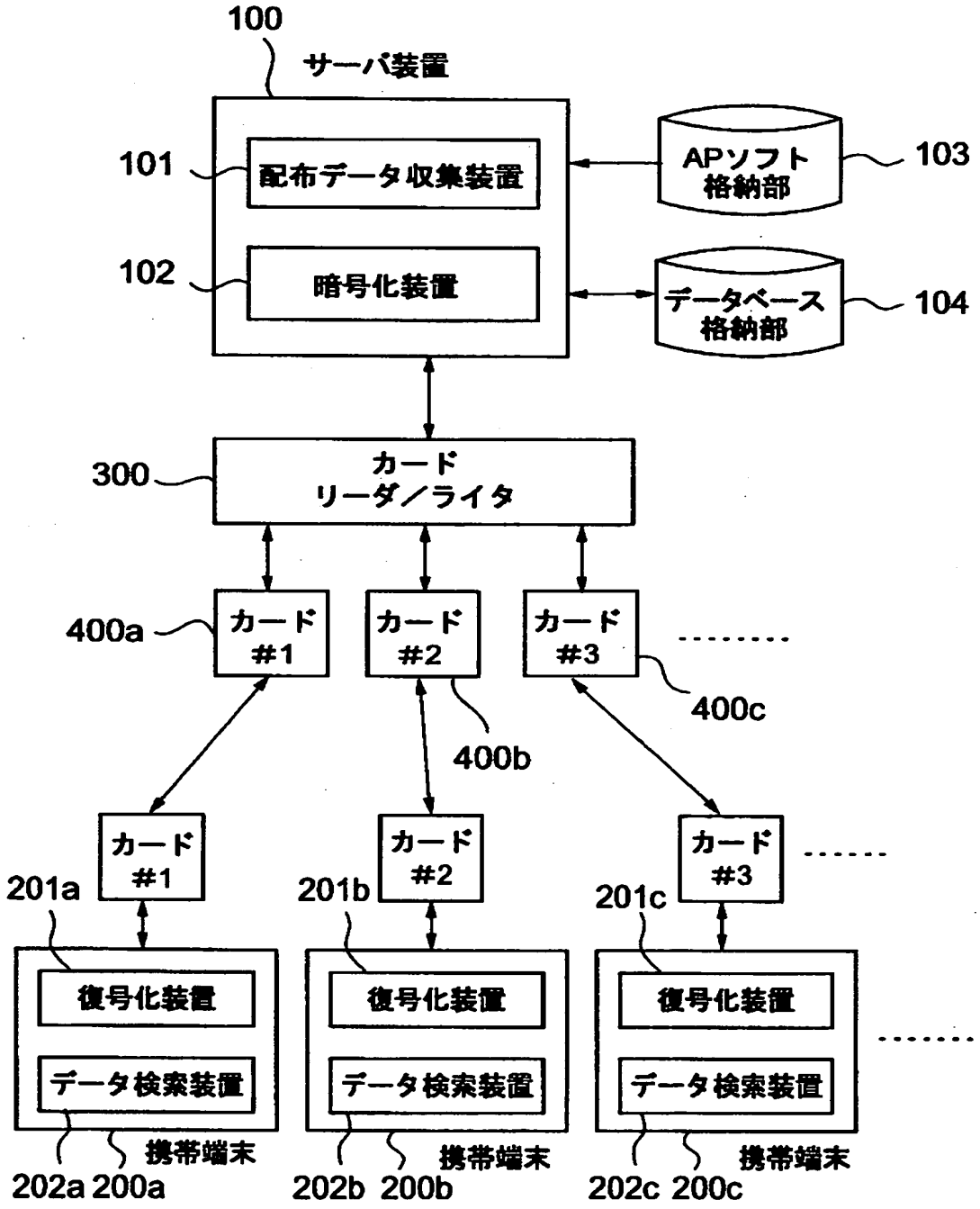
code	name	state	age	phone	line key
1001	wJls	noevjolc	jh	igdltyrfhDSk	9658
1002	ddGGa	h*/fDD	hg	LKtYfDSkoKow	9143
1003	1jkjl+P	gah{6xpVd	tY	hkliiydageQk	8278
1004	3eK@s	kHHS	Kl	d+fDlKnBrtJf	4358
1005	erlN	noevjolc	Gv	wsdERfvW2Sdf	5784
1006	F>sSlu	kHHS	ij	1xcVlmFmkjpo	9743
1007	{:ld?k	lJHFD	LK	kjwDkJGvfDoa	3935
1008	rhJKd	h*/fDD	jh	e419h-ka+qwH	7412
1009	ifd	ASoChijlO-	tY	qLFUjCVkj@kl	9593

復号化 ↓ 列鍵 行鍵

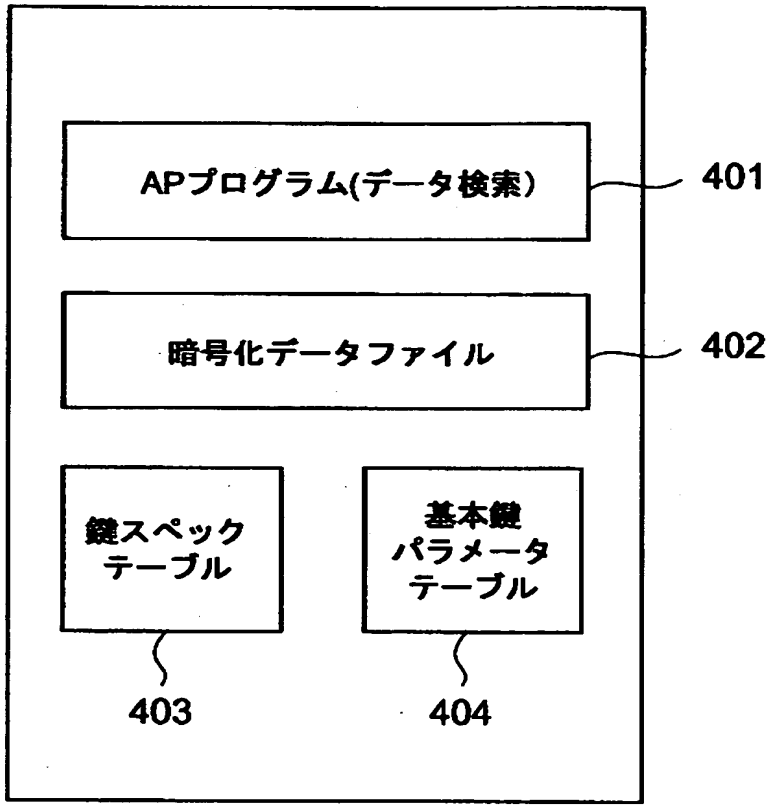
(c)

code	name	state	age	phone
1001	Jhon	New York	22	407-228-6611
1002	Chris	Florida	21	123-456-7890
1003	Michael	Minnesota	27	101-202-3030
1004	David	Iowa	34	523-761-0045
1005	Mark	New York	30	832-962-9001
1006	Daniel	Iowa	25	231-981-9454
1007	George	Idaho	31	561-545-4389
1008	Henry	Florida	22	239-203-9800
1009	Joe	New Jersey	27	239-129-9898

【図１２】


100
サーバ装置
101
配布データ収集装置
102
暗号化装置
APソフト
格納部
103
データベース
格納部
104
300
カード
リーダ／ライタ
400a
カード
#1
カード
#2
カード
#3
400b
400c
201a
201b
201c
復号化装置
データ検索装置
携帯端末
202a
200a
202b
200b
202c
200c

【図１３】


APプログラム(データ検索)
401
暗号化データファイル
402
鍵スペック
テーブル
基本鍵
パラメータ
テーブル
403
404

【書類名】　　要約書

【要約】

【課題】データベース上の特定のデータ項目に対するセキュリティを他のデータ項目よりも高めて暗号化する。

【解決手段】外部データベース記憶装置１８に記憶されたデータベースをデータベースＩ／Ｆ１７を介して読み込む。ここで、鍵スペックテーブル１６ｃを参照してデータベースの所定の列項目のデータについて当該列項目に共通の列鍵を用いて暗号化し、その他の列項目のデータについては高セキュリティが要求される項目として各行毎に固有の行鍵を用いて暗号化する。さらに、基本鍵記憶部１６ｂを参照して前記行鍵を基本鍵にて暗号化し、前記暗号化されたデータベースと共に暗号化データ格納部１６ｄに格納する。このように、各行毎に鍵を異ならせて暗号化し、さらに、当該列項目の暗号化に用いられた鍵を別の鍵で再暗号化することで、鍵の解読を困難として高セキュリティ化を実現することができる。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　　〔０００００１４４３〕

１．変更年月日　　１９９８年　１月　９日
［変更理由］　住所変更
住　所　東京都渋谷区本町１丁目６番２号
氏　名　カシオ計算機株式会社